UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/607,195	06/25/2003	Terence Spies	ID-7	5788

36532 7590 11/10/2004

G. VICTOR TREYZ
FLOOD BUILDING
870 MARKET STREET, SUITE 984
SAN FRANCISCO, CA 94102

EXAMINER	
CHEN, SHIN HON	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 11/10/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/607,195	SPIES ET AL.	
	Examiner	Art Unit	
	Shin-Hon Chen	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 October 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *20031014*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-24 have been examined.

Claim Objections

2. Claim 10 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. The claims that claim 10 depend on do not disclose a certificate authority provides a certificate that contains the service name of the IBE parameter information host.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-3, 5-9, 11-17, 19-22, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant's Admitted Prior Art (hereinafter AAPA) in view of Mont "The HP Time Vault Service: Innovating the Way Confidential Information is Disclosed, at the Right Time" (hereinafter Mont) and further in view of Smith et al. U.S. Pat. No. 6061448 (hereinafter Smith) and further in view of Lee U.S. Pub. No. 20020188690 (hereinafter Lee).

5. As per claim 1, AAPA discloses a method for using identity-based encryption (IBE) to securely convey messages over a communications network from a sender to a recipient, wherein the recipient has an associated IBE public key and an associated IBE private key for use in IBE encryption and decryption, wherein the sender uses the IBE public key of the recipient and IBE public parameter information associated with the recipient, wherein the IBE public parameter information is maintained on an IBE public parameter information is maintained on an IBE public parameter information host that provides the IBE public parameter information over the communications network, wherein the host has a service name that is used to communicate with the host over the network (AAPA: pages 1-3: the IBE system and use of public key and public parameter information to encrypt message). AAPA does not explicitly disclose the method comprising: at the sender, using a service name generation rule to generate the service name of the host based on the IBE public key of the recipient; using the service name to obtain the IBE public parameter information associated with the recipient for the sender from the IBE public parameter host over the network; and at the sender, using the IBE public parameter information obtained from the IBE public parameter host and the IBE public key of the recipient to encrypt a message for the recipient. However, Mont discloses contacting the TA site to retrieve the public parameter information so that the sender can encrypt the message to be sent to the recipient (Mont: page 9 and page 11). One with ordinary skill in the art would use both public key of the recipient and the public detail/parameter from Trusted Authority to encrypt message to be sent to recipient. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Mont within the system of AAPA because the public detail/parameter is used to provide functionality of a trusted party so that the recipient can

trust that the message came from an authentic source. AAPA does not explicitly disclose the public parameter can be retrieved from a host associated with the recipient's public key. However, Smith discloses that public key can be requested from Delivery Server (Smith: column 2 line 65 – column 3 line 32). Since Mont discloses that the public key of recipient can be e-mail address, the sender can request public key from the mail delivery server (host) and use the public key to encrypt messages to be sent to recipient. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Smith within the combination of AAPA-Mont because using the public key of trusted authority to encrypt message increases the authenticity and security of the message. AAPA as modified does not explicitly disclose generating a host name associated with the public key. However, Lee discloses using the e-mail address of the recipient to trace the e-mail server so that certain functions can be performed (Lee: [0022]; [0028]-[0034]). One with ordinary skill in the art at the time of applicant's invention would use the e-mail address (public key) to generate the e-mail server address so that the server address can be obtained to request the public key required to encrypt message to be sent to recipient. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Lee within the combination of AAPA-Mont-Smith because it allows the sender to check whether the address for the intended recipient exists and whether the address and domains are correct.

6. As per claim 2, AAPA as modified discloses the method defined in claim 1. AAPA as modified further discloses the method comprising: at the sender, using the service name generated with the service generation rule and the IBE public key to provide the host with a

request that the host provide the IBE public parameter information to the sender (Lee: [0022]; [0028]-[0034]: generate the host address); and with the IBE public parameter host, providing the IBE public parameter information to the sender in response to the request for the IBE public parameter information from the sender (Smith: column 2 line 65 – column 3 line 32). Same rationale applies here as above in rejecting claim 1.

7. As per claim 3, AAPA as modified discloses the method defined in claim 2. AAPA as modified further discloses the method comprising: at the sender, sending the request to the host server (Smith: column 2 line 65 – column 3 line 32). AAPA does not explicitly disclose sending e-mail message to request public key. However, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to communicate using e-mail message, instant message, or packets within communication network to retrieve desired information.

8. As per claim 5, AAPA as modified discloses the method defined in claim 1. AAPA as modified further discloses wherein the recipient has a message address, the method further comprising: at the sender, using the service name generation rule to generate the service name of the IBE public parameter host (Lee: [0022]; [0028]-[0034]). AAPA as modified does not explicitly disclose generating host name by prepending a string to at least a portion of the message address. However, since the purpose of generating the host name is to contact the e-mail server. Therefore, it would have been obvious to one having ordinary skill in the art to modify the teachings of Lee to prepend the e-mail server name to a portion of the recipient's e-mail

address (e.g. the domain section) to generate a server address and contact e-mail server for information. Since the applicant has not disclosed generating the host/server address by prepending the server/host name to the domain section of an e-mail address solves any specific problem or for any particular purpose, it appears generating the address of the e-mail server/host by examining the domain portion and searching for server address would work equally well.

9. As per claim 6, claim 6 encompasses the same scope as described in claim 5. Therefore, claim 6 is rejected based on the reason set forth in claim 5.

10. As per claim 7, AAPA as modified discloses the method defined in claim 1. AAPA as modified further discloses wherein the IBE public parameter information host has an identity, the method further comprising: at the sender, verifying the identity of the IBE public parameter information host from which the IBE public parameter information is obtained (Lee: [0022], [0028]-[0034]: host name checker). It would have been obvious to one having ordinary skill in the art at the time of invention to check the sender's identity of the e-mail host so that proper message can be delivered. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Lee within the combination of AAPA-Mont-Smith-Lee because it reduces the likelihood of sending e-mail to an address that does not exist.

11. As per claim 8, AAPA as modified discloses the method defined in claim 7. AAPA as modified further discloses wherein verifying the identity of the IBE public parameter information

host comprises: at the sender, comparing service name information received from the IBE public parameter information host by the sender to the service name generated with the service name generation rule to determine whether there is a match (Lee: [0022], [0028]-[0034]: checks whether a host name input by the user exists). Same rationale applies here as above in rejecting claim 7.

12. As per claim 9, AAPA as modified discloses the method defined in claim 7. AAPA as modified further discloses wherein the IBE public key of the recipient includes a message address having a domain name portion and wherein verifying the identity of the IBE public parameter information host comprises: at the sender, comparing identity information received from the IBE public parameter information host by the sender to the domain name portion of the message address to determine whether the identity information matches the domain name portion (Lee: [0022], [0028]-[0034]: checks whether a host name input by the user exists). Same rationale applies here as above in rejecting claim 7.

13. As per claim 11, AAPA as modified discloses the method defined in claim 1. AAPA as modified further discloses the method comprising: with the IBE public parameter information host, providing the sender with identity information signed by a certificate authority (Smith: column 2 line 65 – column 3 line 32).

14. As per claim 12, AAPA as modified discloses the method defined in claim 1. AAPA as modified further discloses the method comprising, with the IBE public parameter information

host, providing the sender with the IBE public parameter information signed by a certificate authority (Smith: column 2 line 65 – column 3 line 32).

15. As per claim 13 and 14, AAPA as modified discloses the method defined in claim 1. AAPA as modified further discloses wherein providing the IBE public parameter information to the sender comprises providing the IBE public parameter information to the sender over a secure/insecure communications link (Smith: column 5 lines 60-63: communicate with the delivery server through secure channel). It would have been obvious to one having ordinary skill in the art to use either secure/insecure communications link to transfer data depending on whether the data is confidential because the encrypted data can be sent through insecure channel and unencrypted data can be sent through secure channel and both being received securely.

16. As per claim 15, AAPA as modified discloses the method defined in claim 14. AAPA as modified does not explicitly disclose wherein providing the IBE public parameter information to the sender over the insecure link comprises using the IBE public parameter information host to encrypt the IBE public parameter in a message format prior to sending the IBE public parameter information to a sender in the message format over the insecure link. However, transferring confidential data over insecure channel by encrypting the confidential data before transmission is well known in the art. Therefore, one with ordinary skill in the art would encrypt a confidential data first before sending it through insecure communication link.

17. As per claim 16, 19, 21, 22, and 24, claims 16, 19, 21, 22, and 24 encompass the same scope as disclosed in claim 1. Therefore, claims 16, 19, 21, 22, and 24 are rejected based on the same reason set forth in claim 1.

18. As per claim 17, AAPA as modified discloses the method defined in claim 1. AAPA as modified does not explicitly disclose wherein the message is an instant message and wherein the IBE public key of the recipient comprises an instant message address, the method comprising: at the sender, using the instant message address of the recipient to send the instant message to the recipient over the communications network. However, one with ordinary skill in the art would apply the method over any communications method not limiting to e-mail and instant message.

19. As per claim 20, AAPA as modified discloses the method defined in claim 1. AAPA as modified does not explicitly disclose the method further comprises a domain name, the method further comprising: at the sender, using the domain name to establish a secure sockets layer communications link with the IBE public key parameter information host over the Internet. However, SSL is well known in the art to establish secure communication path in Internet communications because it supports authentication of client, server, or both, as well as encryption during a communications session.

20. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over AAPA in view of Mont and further in view of Smith and further in view of Lee and further in view of Boneh et al. U.S. Pub. No. 20030081785 (hereinafter Boneh).

21. As per claim 4, AAPA as modified discloses the method defined in claim 1. AAPA as modified does not explicitly discloses wherein an IBE private key generator is connected to the network, the method further comprising: electronically conveying the IBE public parameter information from the IBE private key generator to the host. However, Boneh discloses the private key generator generate public parameter for message sender (Boneh: [0059] and [0064]). It would have been obvious to one having ordinary skill in the art to interpret the PKG as trusted authority that generate public parameter and private key for the identity based encryption system and the trusted authority provide the public key/public parameter to host/server as disclosed by Smith (column 2 line 65 – column 3 line 32) and retrieved by sender. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Boneh within the combination of AAPA-Mont-Smith-Lee because the PKG serves as a trusted authority in providing authenticity of the message sent by sender through the use of the public parameter and use of PKG within IBE is well known in the art. Furthermore, the PKG can serve as independent entity or an entity within a server/host.

22. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over AAPA in view of Mont and further in view of Smith and further in view of Lee and further in view of McMorris et al. U.S. Pub. No. 20030163567 (hereinafter McMorris).

23. As per claim 10, AAPA as modified discloses the method defined in claim 7. AAPA as modified discloses the Delivery server sends the public key (certificate) to the sender upon request. AAPA as modified does not explicitly disclose wherein a certificate authority provides a

certificate that contains the service name of the IBE public parameter information host and wherein verifying the identity of the IBE public parameter information host comprises: providing the certificate that contains the service name of the IBE public parameter information host to the sender so that the sender can compare signed service name information in the certificate to the service name of the host that was generated by the service name generation rule to determine whether there is a match. However, McMorris discloses comparing the domain name with the domain name in a digital certificate to validate a domain name associated with an attempt to access to a network site (McMorris: figure 3 and [0030]-[0031]: the domain name of hotmail.com in a digital certificate). One with ordinary skill in the art would compare the domain name generated by user (Lee: [0022], [0028]-[0034]) with the domain name in a digital certificate (Smith: column 2 line 65 – column 3 line 32: Delivery server transmits a certificate to mail sender) in order to authenticate users attempting to access network resource. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of McMorris within the combination of AAPA-Mont-Smith-Lee because the comparison allows the system to authenticate users and avoid man-in-the-middle attack by denying access to the secure server when comparison fails.

24. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over AAPA in view of Mont and further in view of Smith and further in view of Lee and further in view of Mont U.S. Pub. No. 20030198348 (hereinafter Mont2).

25. As per claim 18, AAPA as modified discloses the method defined in claim 1. AAPA as modified does not explicitly discloses the method comprising providing the sender with the service name generation rule in a plug-in module. However, Mont2 discloses using plug-in to execute identity based encryption scheme (Mont2: [0021]). One with ordinary skill in the art would use the software plug in to encrypt message and communicate with trust authority using plug in. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Mont2 within the combination of AAPA-Mont-Smith-Lee because software plug in is well known in the art to communicate data in a distributed network environment.

26. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over AAPA in view of Mont and further in view of Smith and further in view of Lee and further in view of Martija et al. U.S. Pub. No. 20020169857 (hereinafter Martija).

27. As per claim 23, AAPA as modified discloses the method defined in claim 1. AAPA as modified does not explicitly disclose wherein the IBE public key contains at least one geographical region attribute, the method further comprising using the service name generation rule to generate the service name by basing the service name at least partially on the geographical region attribute. However, Martija discloses parsing the host name to determine the geographical regions of the host (Martija: [0044]-[0045]). One with ordinary skill in the art would parse the string to obtain information related to domain and geographic regions contain in the string to determine information about the host including generating host name. Therefore, it

would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Martija within the combination of AAPA-Mont-Smith-Lee because parsing a string to determine host domain information is well known in the art.

Conclusion

28. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Gentry et al. U.S. Pub. No. 20030182554 discloses authenticated ID-Based cryptosystem with no key escrow.

Gentry et al. U.S. Pub. No. 20030179885 discloses hierarchical identity-based encryption and signature schemes.

Forman U.S. Pub. No. 20030120733 discloses e-mail system that allows sender to check recipient's status before sending an e-mail to the recipient.

Aravamudan et al. U.S Pat. No. 6396830 discloses implementing network services over the Internet through dynamic resolution of personal host names.

Bouchard U.S. Pub. No. 20030115448 discloses methods and apparatus for securely communicating a message.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (703) 305-8654. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shin-Hon Chen
Examiner
Art Unit 2131

SC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100